⑲日本国特許庁(JP)　⑩特許出願公開

⑫公開特許公報(A)　平2-44389

⑤Int.Cl.⁵	識別記号	庁内整理番号
G 09 C 1/00		7368-5B
G 06 K 17/00	S	6711-5B
19/10		6711-5B

⑬公開　平成2年(1990)2月14日

G 06 K 19/00　R

審査請求　未請求　請求項の数 3　(全9頁)

⑤④発明の名称　ICカード機器

⑳特　願　昭63-194988

㉒出　願　昭63(1988)8月4日

㉗発明者　伊藤　守　大阪府門真市大字門真1006番地　松下電器産業株式会社内

㉗発明者　高木　伸哉　大阪府門真市大字門真1006番地　松下電器産業株式会社内

㉑出願人　松下電器産業株式会社　大阪府門真市大字門真1006番地

㉔代理人　弁理士　粟野　重孝　外1名

明　細　書

1、発明の名称

ICカード機器

2、特許請求の範囲

(1) 第1のICカード装置と、この第1のICカード装置と交信する第2のICカード装置とを備え、前記第1のICカード装置は、乱数を発生するための第1の乱数発生手段と、前記第1の乱数発生手段から得られる乱数を暗号化するための第1の暗号化手段と、外部から入力される暗号化データを復号化するための第2の復号化手段と、前記第2の復号化手段から得られるデータを第1のデータと第2のデータに分離するためのデータ分離手段と、前記データ分離手段から得られる第2のデータを暗号化するための第3の暗号化手段と、前記第1の乱数発生手段から得られる乱数と前記データ分離手段から得られる第1のデータを比較するための第1の比較手段と、データの入出力、記憶、演算などのデータ処理を行なう第1の処理手段と、前記データ分離手段から得られる第2のデータと前記第1の乱数発生手段から得られる乱数を用いて前記第1の処理手段から送出されるデータを暗号化し、外部から入力される暗号化データを復号化するための第1の通信手段とを有し、前記第2のICカード装置は、乱数を発生するための第2の乱数発生手段と、外部から入力される暗号化データを復号化するための第1の復号化手段と、前記第2の乱数発生手段から得られる乱数と前記第1の復号化手段から得られるデータを連結するためのデータ連結手段と、前記データ連結手段から得られる連結データを暗号化するための第2の暗号化手段と、外部から入力される暗号化データを復号化するための第3の復号化手段と、前記第2の乱数発生手段から得られる乱数と前記第3の復号化手段から得られるデータを比較するための第2の比較手段と、データの入出力、記憶、演算などのデータ処理を行なう第2の処理手段と、前記第1の復号化手段から得られるデータと前記第2の乱数発生手段から得られる乱数を用いて外部から

入力される暗号化データを復号化し、前記第２の処理手段から送出されるデータを暗号化するための第２の通信手段とを有する構成としたＩＣカード機器。

(2) 第１のＩＣカード装置に装着される第３のＩＣカード装置は、第１の乱数発生手段と第１の暗号化手段と第２の復号化手段と第３の暗号化手段とデータ分離手段と第１の比較手段から構成される請求項１記載のＩＣカード機器。

(3) 第２のＩＣカード装置に装着される第４のＩＣカード装置は、第２の乱数発生手段と第１の復号化手段と第２の暗号化手段と第３の復号化手段とデータ連結手段と第２の比較手段から構成される請求項１記載のＩＣカード機器。

３、発明の詳細な説明

産業上の利用分野

本発明は、第１のＩＣカード装置（例えば主として情報を記憶する集積回路がカード内に組み込まれたＩＣカード）と、そのＩＣカードと情報の交換を行う第２のＩＣカード装置（例えばカード端末）とから構成されるＩＣカード機器に関するものである。

従来の技術

第４図は従来例を示したものである。

第４図において、カード端末４００は、乱数Ｒを生成するための乱数発生手段４０１と、第１の秘密データＫ１と前記乱数発生手段４０１から得られる乱数Ｒと関数演算Ｆ１を行うための第１の演算手段４０２と、前記第１の演算手段４０２から得られるデータとＩＣカード４５０から入力されるデータとを比較するための比較手段４０３と、データの入出力、記憶、演算などのデータ処理を行う第１の処理手段４０６と、第１の暗号化鍵ＫＥ１を用いて前記第１の処理手段４０６から送出されるデータを暗号化するための第１の暗号化手段４０４と、第２の復号化鍵ＫＤ２を用いてＩＣカード４５０から入力される暗号化データを復号化するための第２の復号化手段４０５とを備えている。一方、カード端末４００と情報の交換を行うＩＣカード４５０は、第２の秘密データＫ２とカード端末４００から入力される乱数Ｒと

の関数演算Ｆ２を行うための第２の演算手段４５２と、データの入出力、記憶、演算などのデータ処理を行う第２の処理手段４５６と、第１の復号化鍵ＫＤ１を用いてカード端末４００から入力される暗号化データを復号化するための第１の復号化手段４５４と、第２の暗号化鍵ＫＥ２を用いて前記第２の処理手段４５６から送出されるデータを暗号化するための第２の暗号化手段４５５とを備えている。

このように構成された従来のＩＣカード機器について、その動作を以下に説明する。

ＩＣカード４５０がカード端末４００に挿入されると情報の交換を行う前に、カード端末４００はＩＣカード４５０の正当性（偽造されていないこと）を確認するため、乱数発生手段４０１から乱数Ｒを生成し、ＩＣカード４５０に送信する。ＩＣカード４５０が受信した乱数Ｒは第２の演算手段４５２に入力され、ＩＣカード４５０内に記憶されている第２の秘密データＫ２とあらかじめ定められた関数演算Ｆ２が施されてカード端末４００に送信され、カード端末４００内の比較手段４０３に入力される。

一方、カード端末４００ではＩＣカード４５０と同様に、乱数発生手段４０１から得られる乱数Ｒは第１の演算手段４０２に入力され、カード端末４００内に記憶されている第１の秘密データＫ１とあらかじめ定められた関数演算Ｆ１が施され、比較手段４０３に入力される。第１と第２の演算手段４０２，４５２が同一の関数演算を行い、第１と第２の秘密データが同一のデータであれば、比較手段４０３に入力される二つのデータは同一の値を持つ。比較手段４０３は、入力された二つのデータを比較し、両者が一致している時に限り、カード端末４００はＩＣカード４５０を正当なＩＣカードであると判断して、第１の処理手段４０６に対してＩＣカード４５０との情報の交換を許可する。

情報の交換を許可された第１の処理手段４０６は第１の暗号化手段４０４に対して送信データを送出し、第１の暗号化手段４０４はカード端末

４００に記憶されている第１の暗号化鍵ＫＥ１を用い、入力された送信データを暗号化してＩＣカード４５０に送信する。ＩＣカード４５０が受信した暗号化データは第１の復号化手段４５４に入力され、ＩＣカード４５０内に記憶されている第１の復号化鍵ＫＤ１を用いて復号化され、第２の処理手段４５６に入力される。

また、第２の処理手段４５６は第２の暗号化手段４５５に送信データを送出し、第２の暗号化手段４５５はＩＣカード４５０内に記憶されている第２の暗号化鍵ＫＥ２を用いて暗号化し、カード端末４００に送信する。カード端末４００が受信した暗号化データは第２の復号化手段４０５に入力され、カード端末４００内に記憶されている第２の復号化鍵ＫＤ２を用いて復号化され、第１の処理手段４０６に入力される。以上のように、暗号化処理と復号化処理の繰り返しにより、カード端末４００とＩＣカード４５０との間で情報の交換が行われる。

発明が解決しようとする課題

また、情報の交換については、あらかじめカード端末４００とＩＣカード４５０に記憶されている暗号化鍵と復号化鍵を用いて、交換しようとする情報の暗号化処理と復号化処理を行いながらカード端末４００とＩＣカード４５０間で通信を行うため、暗号化処理と復号化処理において同一の暗号アルゴリズムと同一の鍵が長期間使用されると暗号が解読され、通信情報が漏洩する危険性があった。

これらの問題点を解決するためには、カード端末４００とＩＣカード４５０の両方に記憶されている秘密データや暗号化鍵、復号化鍵を頻繁に取り換える必要があるが、ＩＣカード４５０は不特定多数のユーザに所持されることが多いため、現実的には秘密データや暗号化鍵、復号化鍵の取り換えはかなり困難である。

本発明はこのような課題に鑑み、秘密データや暗号化鍵、復号化鍵を頻繁に取り換えることなく、ＩＣカードの正当性が確認でき、また、安全にＩＣカードとカード端末の間で情報の交換が行なえるようなＩＣカード機器を提供することを目的としている。

このような従来のＩＣカード機器において、まずＩＣカード４５０がカード端末４００の正当性を確認できないという問題点があった。この問題点については、ＩＣカード４５０がカード端末４００と同様な乱数発生手段と比較手段とを具備すれば、カード端末４００がＩＣカード４５０の正当性を確認する方法と同様にＩＣカード４５０がカード端末４００の正当性を確認することができ、容易に解決することができる。

しかしながら、このような従来のＩＣカード機器においては、カード端末４００がＩＣカード４５０の正当性を確認するために生成した乱数Ｒと、その乱数Ｒを第２の演算手段４５２で演算した結果Ｆ２（Ｒ，Ｋ２）とが端末とＩＣカードのインタフェース部に毎回あらわれるため、第三者が乱数Ｒとその演算結果Ｆ２（Ｒ，Ｋ２）のペアを容易に入手することが可能となり、万一、関数演算のアルゴリズムが漏洩すると、秘密データが解読される恐れがあり、ＩＣカードが偽造される危険性があった。

課題を解決するための手段

上記目的を達成するため、本発明は、第１のＩＣカード装置は、乱数を発生するための第１の乱数発生手段と、前記第１の乱数発生手段から得られる乱数を暗号化するための第１の暗号化手段と、外部から入力される暗号化データを復号化するための第２の復号化手段と、前記第２の復号化手段から得られるデータを第１のデータと第２のデータに分離するためのデータ分離手段と、前記データ分離手段から得られる第２のデータを暗号化するための第３の暗号化手段と、前記第１の乱数発生手段から得られる乱数と前記データ分離手段から得られる第１のデータを比較するための第１の比較手段と、データの入出力、記憶、演算などのデータ処理を行う第１の処理手段と、前記データ分離手段から得られる第２のデータと前記第１の乱数発生手段から得られる乱数を用いて前記第１の処理手段から送出されるデータを暗号化

し、外部から入力される暗号化データを復号化するための第１の通信手段とを備えたものとし、第２のＩＣカード装置は、乱数を発生するための第２の乱数発生手段と、外部から入力される暗号化データを復号化するための第１の復号化手段と、前記第２の乱数発生手段から得られる乱数と前記第１の復号化手段から得られるデータを連結するためのデータ連結手段と、前記データ連結手段から得られる連結データを暗号化するための第２の暗号化手段と、外部から入力される暗号化データを復号化するための第３の復号化手段と、前記第２の乱数発生手段から得られる乱数と前記第３の復号化手段から得られるデータを比較するための第２の比較手段と、データの入出力、記憶、演算などのデータ処理を行なう第２の処理手段と、前記第１の復号化手段から得られるデータと前記第２の乱数発生手段から得られる乱数を用いて外部から入力される暗号化データを復号化し、前記第２の処理手段から送出されるデータを暗号化するための第２の通信手段とを備えたものにしたものである。

作用

本発明は上記した構成により、第２のＩＣカード装置（例えばＩＣカードで以下、ＩＣカードと記する）が第１のＩＣカード装置（例えばカード端末で以下、カード端末と記する）に挿入されると、カード端末は乱数データを生成し、これをカード端末内にあらかじめ記憶されている暗号化鍵で暗号化してＩＣカードに送信する。ＩＣカードは受信した暗号化データをＩＣカード内にあらかじめ記憶されている復号化鍵で復号化し、カード端末が生成した乱数データと同一であると推定される乱数データを得る。さらに、ＩＣカードはＩＣカード内でも乱数データを生成し、生成した乱数データとカード端末が送信してきた乱数データとを連結し、ＩＣカード内にあらかじめ記憶されている暗号化鍵で暗号化してカード端末に送信する。

カード端末は、受信した暗号化データをあらかじめカード端末内に記憶されている復号化鍵を用いて復号化し、連結データを得る。カード端末はこの連結データを二つの乱数データに分離し、このうちＩＣカードが生成したと推定される乱数データをあらかじめカード端末に記憶されている暗号化鍵で暗号化してＩＣカードに送信し、一方のカード端末が生成したと推定される乱数データをカード端末が実際に生成した乱数データと比較する。また、ＩＣカードは、受信した暗号化データをあらかじめＩＣカード内に記憶されている復号化鍵で復号化し、この復号化データをＩＣカードが実際に生成した乱数データと比較する。

カード端末において、カード端末が生成したと推定される乱数データとカード端末が実際に生成した乱数データとが一致するためには、カード端末が生成した乱数データがＩＣカード内で正しく復号化及び暗号化される必要があり、こういう処理が可能なＩＣカードは正当な手段で配送された復号化鍵と暗号化鍵を有していると考えられ、カード端末にとって正当なＩＣカードであると判断できる。またＩＣカードにおいて、カード端末から受信し復号化したデータとＩＣカードが実際に生成した乱数データとが一致するためには、ＩＣカードが生成した乱数データがカード端末内で正しく復号化及び暗号化される必要があり、こういう処理が可能なカード端末は正当な手段で配送された復号化鍵と暗号化鍵を有していると考えられ、ＩＣカードにとって正当な端末であると判断してよい。

このとき、カード端末とＩＣカードのインタフェース部には、カード端末とＩＣカードが生成した二つの乱数データをそれぞれ暗号化したものと前記二つの乱数データを連結したデータを暗号化したものしかあらわれない。従って、第三者にこれらの暗号化データが入手されても、カード端末もしくはＩＣカードで生成される乱数データが入手できないため、暗号化鍵を推定するのはきわめて困難であり、長期間にわたって同一の暗号化鍵を使用することができる。

以上のプロセスによりＩＣカードとカード端末の互いの正当性が確認されると、カード端末と

ＩＣカードはそれぞれが生成し、秘密に交換した二つの乱数データを用いて互いに暗号化処理と復号化処理を繰り返しながら、カード端末とＩＣカードの間で暗号による情報の交換を行う。ＩＣカードがカード端末に挿入されるたびに生成される乱数データを暗号化鍵と復号化鍵に用いているため、鍵を頻繁に取り換えることなく安全に情報の交換を行うことができる。

実施例

以下本発明の実施例について、図面を参照しながら説明する。

（実施例１）

第１図は、本発明のＩＣカード端末装置の第１の実施例を示すブロック図である。

第１図において、１１０はカード端末１００に挿入された取引用ＩＣカード１５０の正当性を確認するためにカード端末１００内に装着された認証用ＩＣカードである。１１１は乱数データＲＯを発生するための第１の乱数発生手段、１１２は認証用ＩＣカード１１０内に記憶されている第１の暗号化鍵ＫＥ１を用いて前記第１の乱数発生手段１１１から得られる乱数データＲＯを暗号化するための第１の暗号化手段である。１１３は認証用ＩＣカード１１０内に記憶されている第２の復号化鍵ＫＤ２を用いて外部から入力される暗号化データを復号化するための第２の復号化手段、１１５は前記第２の復号化手段１１３から得られるデータを第１のデータＲ２と第２のデータＳ１に分離するためのデータ分離手段である。１１４は認証用ＩＣカード１１０内に記憶されている第３の暗号化鍵ＫＥ３を用いて前記データ分離手段１１５から得られる第２のデータＳ１を暗号化するための第３の暗号化手段である。１１６は前記第１の乱数発生手段１１１から得られる乱数データＲＯと前記データ分離手段１１５から得られる第１のデータＲ２を比較するための第１の比較手段である。１２０はデータの入出力、記憶、演算などのデータ処理を行う第１の処理手段である。１３０は前記データ分離手段１１５から得られる第２のデータＳ１と前記第１の乱数発生手段１１１から得られる乱数データＲＯを用いて前記第１の処理手段１２０から送出されるデータを暗号化し、外部から入力される暗号化データを復号化するための第１の通信手段で、以上から第１のＩＣカード装置としてのカード端末１００が構成されている。なお、第１の乱数発生手段１１１と第１の暗号化手段１１２と第２の復号化手段と第３の暗号化手段１１４とデータ分離手段１１５と第１の比較手段１１６とは、認証用ＩＣカード１１０内に構成され、カード端末１００の一部として機能している。

また、１５１は乱数データＳＯを発生するための第２の乱数発生手段、１５２は取引用ＩＣカード１５０内に記憶されている第１の復号化鍵KD1を用いて外部から入力される暗号化データを復号化するための第１の復号化手段である。１５５は前記第２の乱数発生手段１５１から得られる乱数データＳＯと前記第１の復号化手段１５２から得られるデータＲ１を連結するためのデータ連結手段、１５１は取引用ＩＣカード１５０内に記憶されている第２の暗号化鍵ＫＥ２を用いて前記データ連結手段１５５から得られる連結データを暗号化するための第２の暗号化手段である。１５４は取引用ＩＣカード１５０内に記憶されている第３の復号化鍵ＫＤ３を用いて外部から入力される暗号化データを復号化するための第３の復号化手段、１５６は前記第２の乱数データ発生手段１５１から得られる乱数データＳＯと前記第３の復号化手段１５４から得られるデータＳ２を比較するための第２の比較手段である。１６０はデータの入出力、記憶、演算などのデータ処理を行う第２の処理手段、１７０は前記第１の復号化手段１５２から得られるデータＲ１と前記第２の乱数発生手段１５１から得られる乱数データＳＯを用いて外部から入力される暗号化データを復号化し、前記第２の処理手段１６０から送出されるデータを暗号化するための第２の通信手段で、以上から第２のＩＣカード装置としての取引用ＩＣカード１５０が構成されている。上記のように構成されたＩＣカード機器について、以下その動作を説明する。

まず、認証用ＩＣカード１１０が装着されたカード端末１００に取引用ＩＣカード１５０が挿入されると、認証用ＩＣカード１１０内の第１の乱数発生手段１１１は乱数データＲ０を生成し、第１の暗号化手段１１２は認証用ＩＣカード１１０にあらかじめ記憶されている第１の暗号化鍵KE1を用いて前記第１の乱数発生手段１１１から得られる乱数データＲ０を暗号化して取引用ＩＣカード１５０に送信する。取引用ＩＣカード１５０内の第１の復号化手段１５２は受信した暗号化データを取引用ＩＣカード１５０内にあらかじめ記憶されている第１の復号化鍵ＫＤ１で復号化し、認証用ＩＣカード１１０が生成した乱数データＲ０と同一であると推定される乱数データＲ１を得る。

次に、取引用ＩＣカード１５０においても第２の乱数発生手段１５１が乱数データＳ０を生成し、データ連結手段１５５は第２の乱数発生手段151から得られる乱数データＳ０と第１の復号化手段１５２から得られる乱数データＲ１との連結処理を行い、連結データＲ１‖Ｓ０を生成する。ここで、「‖」の記号は二つのデータを連結することを意味する。第２の暗号化手段１５３はこの連結データＲ１‖Ｓ０を取引用ＩＣカード１５０内にあらかじめ記憶されている第２の暗号化鍵ＫＥ２を用いて暗号化し、カード端末１００に送信する。

第２の復号化手段１１３はカード端末１００が受信した暗号化データをあらかじめ認証用ＩＣカード１１０内に記憶されている第２の復号化鍵ＫＤ２で復号化し、取引用ＩＣカード１５０が生成したと推定される連結データＲ２‖Ｓ１を得る。データ分離手段１１５はこの連結データを二つの乱数データＲ２，Ｓ１に分離し、第３の暗号化手段１１４は取引用ＩＣカード１５０が生成したと推定される乱数データＳ１をあらかじめ認証用ＩＣカード１１０内に記憶されている第３の暗号化鍵ＫＥ３で暗号化して取引用ＩＣカード１５０に送信し、第１の比較手段１１６は認証用ＩＣカード１１０が生成したと推定される乱数データＲ２と第１の乱数発生手段１１１から得られる実際に生成した乱数データＲ０の値を比較する。

また、第３の復号化手段１５４は取引用ＩＣカード１５０が受信した暗号化データをあらかじめ取引用ＩＣカード１５０内に記憶されている第３の復号化鍵ＫＤ３を用いて復号化し、第２の比較手段１５６は取引用ＩＣカード１５０で生成されたと推定される乱数データＳ２と第２の乱数発生手段１５１から得られる実際に生成した乱数データＳ０の値を比較する。

第１の比較手段１１６において、認証用ＩＣカード１１０が生成したと推定される乱数データＲ２と第１の乱数発生手段１１１から得られる実際に生成した乱数データＲ０との比較結果が第１の処理手段１２０に対する第１の制御信号Ｃ１となる。両データが一致すると、第１の比較手段１１６は第１の処理手段１２０に対して取引用ＩＣカード１５０との情報交換を許可し、不一致のときは情報の交換を禁止する。第２の比較手段１５６においても同様に、取引用ＩＣカード150で生成されたと推定される乱数データＳ２と第２の乱数発生手段１５１から得られる実際に生成した乱数データＳ０との比較結果が第２の処理手段１６０に対する第２の制御信号Ｃ２となり、両データが一致しているときに限り第２の処理手段１６０に対して情報の交換を許可する。

情報の交換が許可された第１の処理手段１２０は第１の通信手段１３０に対して送信データを送出し、第１の通信手段１３０はデータ分離手段１１５から得られる乱数データＳ１と第１の乱数発生手段１１１から得られる乱数データＲ０を用い、入力された送信データを暗号化して取引用ＩＣカード１５０に送信する。取引用ＩＣカード１５０が受信した暗号化データは第２の通信手段１７０に入力され、第１の復号化手段１５２から得られる乱数データＲ１と第２の乱数発生手段１５１から得られる乱数データＳ０を用いて復号化され、第２の処理手段１６０に入力される。

同様に、情報の交換が許可された第２の処理手段１６０は第２の通信手段１７０に対して送信データを送出し、第２の通信手段１７０は第１の復号化手段１５２から得られる乱数データＲ１と第

２の乱数発生手段１５１から得られる乱数データＳ０を用い、入力された送信データを暗号化してカード端末１００に送信する。カード端末１００が受信した暗号化データは第１の通信手段１３０に入力され、データ分離手段１１５から得られる乱数データＳ１と第１の乱数発生手段１１１から得られる乱数データＲ０を用いて復号化され、第１の処理手段１２０に入力される。

以上のように、認証用ＩＣカード１１０と取引用ＩＣカード１５０がそれぞれ生成し、秘密に交換した二つの乱数データを用いて互いに暗号化処理と復号化処理を繰り返すことにより、カード端末１００と取引用ＩＣカード１５０の間で安全に情報の交換を行うことができる。

第３図は、第１の実施例における第１と第２の通信手段の一実施例を示すブロック図である。

第３図において、１３１は第１の処理手段120から送出される送信データを暗号化して取引用ＩＣカード１５０に送信するための第４の暗号化手段、１３２はカード端末１００が受信した暗号化データを復号化し第１の処理手段１２０に入力するための第５の復号化手段で、以上から第１の通信手段１３０が構成されている。また、１７１は取引用ＩＣカード１５０が受信した暗号化データを復号化し第２の処理手段１６０に入力するための第４の復号化手段、１７２は第２の処理手段１６０から送出される送信データを暗号化してカード端末１００に送信するための第５の暗号化手段で、以上から第２の通信手段１７０が構成されている。

第３図の実施例では、第４の暗号化手段１３１と第４の復号化手段１７１に、認証用ＩＣカード１１０で生成された乱数データが暗号化鍵と復号化鍵に用いられ、第５の復号化手段１３２と第５の暗号化手段１７２に、取引用ＩＣカード１５０で生成された乱数データが復号化鍵と暗号化鍵に用いられている。

（実施例２）

第２図は、本発明のＩＣカード端末装置の第２の実施例を示すブロック図である。

第２図において、２００はカード端末、２１０は認証用ＩＣカード、２１１は第２の乱数発生手段、２１２は第１の復号化手段、２１３は第２の暗号化手段、２１４は第３の復号化手段、２１５はデータ分離手段、２１６は第２の比較手段である。２２０は第２の処理手段、２３０は第２の通信手段、２５０は取引用ＩＣカード、２５１は第１の乱数発生手段、２５２は第１の暗号化手段、２５３は第２の復号化手段、２５４は第３の暗号化手段、２５５はデータ分離手段、２５６は第１の比較手段、２６０は第１の処理手段、２７０は第１の通信手段で、以上は第１図の構成と同様なものである。

第１図の構成と異なるのは、認証用ＩＣカード２１０が第２の乱数発生手段２１１と第１の復号化手段２１２と第２の暗号化手段２１３と第３の復号化手段２１４とデータ連結手段２１５と第２の比較手段２１６とから構成され、取引用ＩＣカード２５０が第１の乱数発生手段２５１と第１の暗号化手段２５２と第２の復号化手段２５３と第３の暗号化手段２５４とデータ分離手段２５５と第１の比較手段２５６とから構成されている点である。

上記のように構成されたＩＣカード根器について、以下その動作を説明する。

まず、認証用ＩＣカード２１０が装着されたカード端末２００に取引用ＩＣカード２５０が挿入されると、取引用ＩＣカード２５０内の第１の乱数発生手段２５１は乱数データＲ０を生成し、第１の暗号化手段２５２は第１の暗号化鍵ＫＥ１を用いて第１の乱数発生手段２５１から得られる乱数データＲ０を暗号化し、カード端末２００に送信する。認証用ＩＣカード２１０内の第１の復号化手段２１２はカード端末２００が受信した暗号化データを第１の復号化鍵ＫＤ１で復号化し、取引用ＩＣカード２５０が生成した乱数データＲ０と同一であると推定される乱数データＲ１を得る。

次に、認証用ＩＣカード２１０においても、第２の乱数発生手段２１１が乱数データＳ０を生成し、データ連結手段２１５は第２の乱数発生手段

２１１から得られる乱数データＳ０と第１の復号化手段２１２から得られる乱数データＲ１との連結処理を行い、連結データＳ０‖Ｒ１を生成する。第２の暗号化手段２１３はこの連結データＳ０‖Ｒ１を第２の暗号化鍵ＫＥ２を用いて暗号化し、取引用ＩＣカード２６０に送信する。

第２の復号化手段２５３は受信した暗号化データを第２の復号化鍵ＫＤ２で復号化し、認証用ＩＣカード２１０が生成したと推定される連結データＳ１‖Ｒ２を得る。データ分離手段２５５はこの連結データを二つの乱数データＳ１，Ｒ２に分離し、第３の暗号化手段２５４は認証用ＩＣカード２１０が生成したと推定される乱数データＳ１を第３の暗号化鍵ＫＥ３で暗号化してカード端末２００に送信し、第１の比較手段２５６は取引用ＩＣカード２５０が生成したと推定される乱数データＲ２と第１の乱数発生手段２５１から得られる実際に生成した乱数データＲ０の値を比較する。

また、第３の復号化手段２１４はカード端末２００が受信した暗号化データをあらかじめ第３の復号化鍵ＫＤ３を用いて復号化し、第２の比較手段２１６は認証用ＩＣカード２１０で生成されたと推定される乱数データＳ２と第２の乱数発生手段２１１から得られる実際に生成した乱数データＳ０の値を比較する。

第１と第２の比較手段２５６，２１６において各乱数データの値が一致すると、それぞれ第１と第２の処理手段２６０，２２０に対して情報の交換を許可し、不一致のときには情報の交換を禁止する。各乱数データが一致し情報の交換が許可されると、第１の実施例とまったく同様に、第１と第２の処理手段２６０，２２０は、第１と第２の通信手段２７０，２３０を介して暗号通信による情報の交換を行う。

発明の効果

以上述べてきたように、本発明は、第１と第２のＩＣカード装置に乱数発生手段と暗号化手段と復号化手段を設けることにより、互いの正当性を確認するために生成する乱数を暗号化処理と復号化処理の鍵に用いることができるため、鍵を頻繁に取り換えることなく、安全に第１と第２のＩＣカード装置間で情報の交換を行うことができ、きわめて優れたＩＣカード機器を実現することができる。

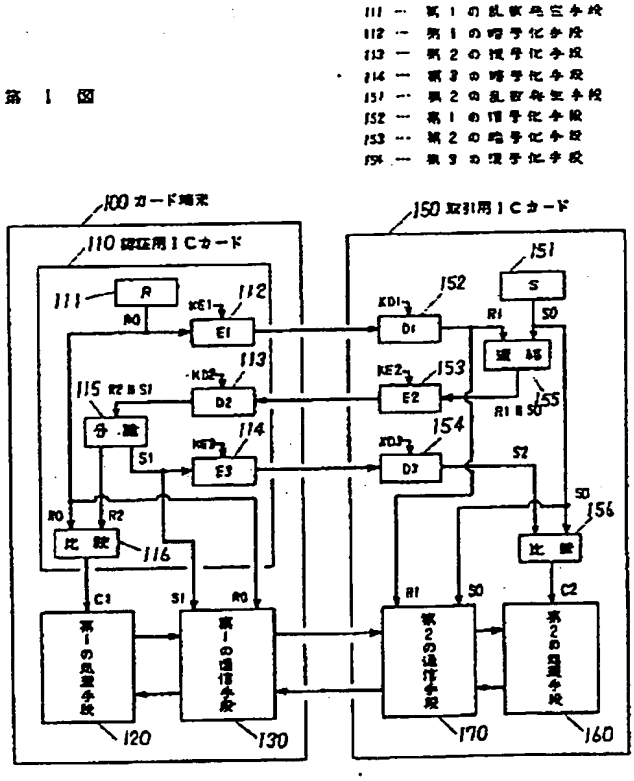
４、図面の簡単な説明

第１図は本発明の第１の実施例におけるＩＣカード機器のブロック図、第２図は本発明の第２の実施例におけるＩＣカード機器のブロック図、第３図は本発明の第１の実施例における通信手段のブロック図、第４図は従来のＩＣカード機器のブロック図である。

１１１……第１の乱数発生手段、１１２……第１の暗号化手段、１１３……第２の復号化手段、１１４……第３の暗号化手段、１５１……第２の乱数発生手段、１５２……第１の復号化手段、１５３……第２の暗号化手段、１５４……第３の復号化手段。

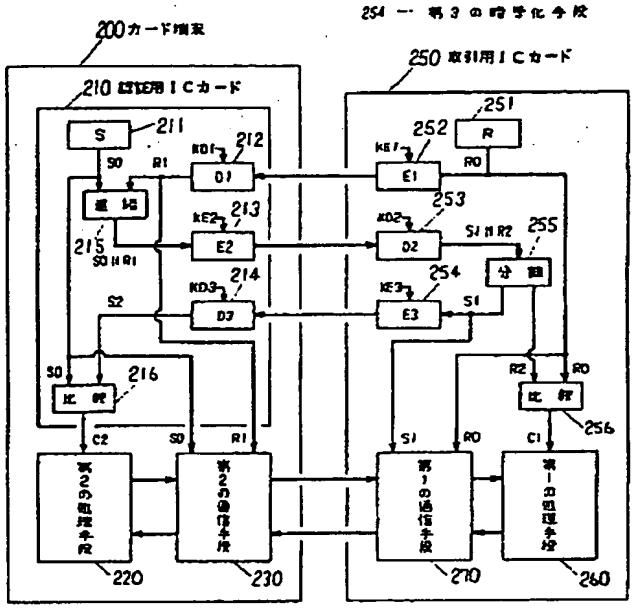
代理人の氏名　弁理士　栗　野　重　孝　ほか１名

第１図



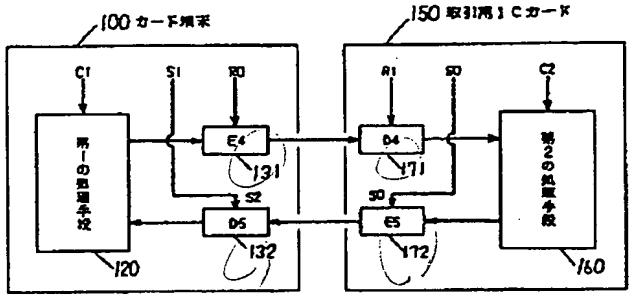
211 — 第2の比較発生手段
212 — 第1の復号化手段
213 — 第2の暗号化手段
214 — 第3の復号化手段
251 — 第1の比較発生手段
252 — 第1の暗号化手段
253 — 第2の復号化手段
254 — 第3の暗号化手段

第 2 図



131 — 第4の暗号化手段
132 — 第5の復号化手段
151 — 第5の暗号化手段
171 — 第4の復号化手段

第 3 図



第 4 図